AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)
The person of DORIAN WOODS

Case No. 3:20MJ422

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

SEE ATTACHMENT A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

SEE ATTACHMENT B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §875(c)	Interstate Threats
18 U.S.C. §372	Conspiracy to impede or injure an officer

The application is based on these facts:

SEE ATTACHED AFFIDAVIT

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Andrea R Kinzig
Applicant's signature

Andrea R. Kinzig, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: 9/10/20

Judge's signature

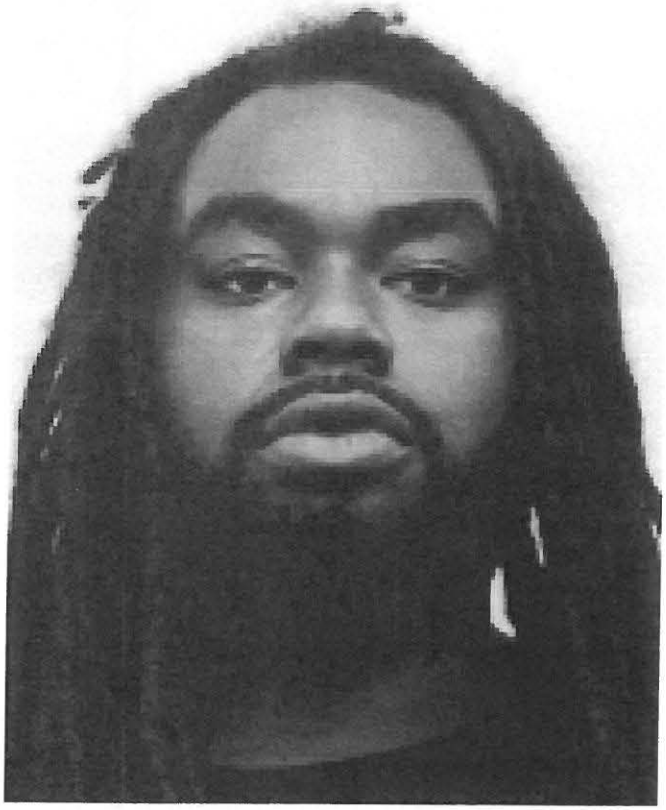
City and state: Dayton, OH

Sharon L. Ovington, U.S. Magistrate Judge
Printed name and title

ATTACHMENT A

DESCRIPTION OF PERSON TO BE SEARCHED

The person of DORIAN WOODS, who is a black male, 26 years old, approximately five feet eleven inches tall, reportedly weighing approximately 280 pounds, having brown hair and brown eyes. The warrant includes authority to search DORIAN WOODS' person and any belongings carried by or in arms' reach of him, such as purses, wallets, bags, containers, and other items.



ATTACHMENT B

Information to be Seized

Items to be Searched for and Seized from the Person Described in Attachment A:

1. Cellular telephones

Search of Electronic Contents of Above-Noted Items:

The above-noted items will be seized, and its electronic records and contents (to include information stored in any form) will be searched at another location for evidence of interstate threats, in violation of 18 U.S.C. §875(c), and conspiracy to impede or injure an officer, in violation of 18 U.S.C. §372, including the following:

1. Any communications regarding the planning, execution, and/or concealment of any threats to harm officers of the Dayton Police Department;

2. Any communications about officers of the Dayton Police Department;

3. Any communications regarding the possession, acquisition, and use of weapons used to harm officers of the Dayton Police Department;

4. Any contact / identifying information for individuals involved in the communications about the above noted offenses;

5. Any Internet searches regarding or related to the planning, execution, and/or concealment of any threats made to harm officers of the Dayton Police Department;

6. Any Internet searches for information about officers of the Dayton Police Department;

7. Information regarding the use of Facebook;

8. Any maps, directions, GPS information, IP addresses, and other location information related to the execution of the above noted offenses;

9. Any images and/or videos depicting officers of the Dayton Police Department;

10. Any images and/or videos depicting firearms or other weapons potentially used in the execution of the above noted offenses;

11. Any images and/or videos depicting the surroundings where the above noted criminal activities transpired;

12. Any information related to the identity of the user(s) of the seized cellular telephones.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

AFFIDAVIT IN SUPPORT OF SEARCH WARRANT

I, Andrea R. Kinzig, being duly sworn, depose and state the following:

INTRODUCTION

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI), and have been so employed since 2005. I am currently assigned to the Dayton, Ohio Resident Agency of the Cincinnati Field Office. In connection with my official duties, I investigate violations of federal criminal laws, including offenses pertaining to interstate threatening communications (in violation of 18 U.S.C. § 875).

2. Along with other agents, officers, and investigators of the FBI and Dayton (Ohio) Police Department, I am currently involved in an investigation of interstate threatening communications made by **DORIAN WOODS**. This Affidavit is submitted in support of an Application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant for the following:

   a. The person of **DORIAN WOODS** (hereinafter referred to as "**WOODS**" and more fully described in Attachment A hereto).

3. This Affidavit is submitted in support of an Application for a search warrant for the person of **WOODS** and any cellular telephones located on **WOODS'** person. The purpose of the Application is to seize evidence of violations of the following: 18 U.S.C. §875(c), which make it a crime to transmit a threat in interstate or foreign commerce to kidnap or injure any person, and 18 U.S.C. §372, which make it a crime to conspire to impede or injure an officer. The items to be searched for and seized are described more particularly in Attachment B hereto and are incorporated by reference.

4. As part of the investigation, I have reviewed documentation and reports provided by and discussed information with other agents, officers, and investigators involved in the investigation. For purposes of this Affidavit, I have not distinguished between information of which I have direct knowledge and that of which I have hearsay knowledge.

5. This Affidavit does not contain every fact known to the investigation, but only those deemed necessary to demonstrate sufficient probable cause to support the searches of the person of **WOODS** and any cellular telephones located on **WOODS'** person.

6. As a result of the instant investigation described more fully below, there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law, including 18 U.S.C. §875(c) and 18 U.S.C. §372, are

present on the person of **WOODS** and any cellular telephones located on **WOODS'** person.

PERTINENT FEDERAL CRIMINAL STATUTES

7. 18 U.S.C. §875(c) states that it is a violation for any person to transmit in interstate or foreign commerce any communication containing any threat to kidnap any person or any threat to injure the person of another.

8. 18 U.S.C. §372 states that it is a violation for two or more persons in any State, Territory, Possession, or District to conspire to prevent, by force, intimidation, or threat, any person from accepting or holding any office, trust, or place of confidence under the United States, or from discharging any duties thereof, or to induce by like means any officer of the United States to leave the place, where his duties as an officer are required to be performed, or to injure him in his person or property on account of his lawful discharge of the duties of his office, or while engaged in the lawful discharge thereof, or to injure his property so as to molest, interrupt, hinder, or impede him in the discharge of his official duties.

BACKGROUND INFORMATION

Definitions

9. The following definitions apply to this Affidavit and Attachment B:

   a. "A **"cellular telephone"** (or mobile telephone or wireless telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

   b. A **"digital camera"** is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be

retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. A "**GPS**" navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated "GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

d. An "**Internet Protocol address**", also referred to as an "**IP address**", is a unique numeric address that computers or electronic devices use in order to communicate with each other on a computer network utilizing the Internet Protocol (IP) standard. Every computer or device connected to the Internet is referenced by a unique IP address. An IP address can be thought of as the equivalent to a street address or a phone number, just as each street address and phone number uniquely identifies a building or telephone. IP addresses are composed of four sets of digits known as "octets," ranging in value from 0-255, separated by decimal points. An example of an IP address is 192.168.10.102. There are two types of IP addresses; static and dynamic. A static address is permanently assigned to a particular device and as a practical matter never changes. A dynamic address provided by an Internet service provider to a client computer is valid only for the duration of the session that the client computer is connected to the Internet (or other network).

e. "**Website**" consists of textual pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from web servers to various web clients via Hyper-Text Transport Protocol (HTTP).

f. The terms "**records**," "**documents**," and "**materials**," as used herein, include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including, but not limited to, writings, drawings, painting), photographic form (including, but not limited to, microfilm, microfiche, prints,

slides, negatives, videotapes, motion pictures, photocopies), mechanical form (including, but not limited to, phonograph records, printing, typing) or electrical, electronic or magnetic form (including, but not limited to, tape recordings, cassettes, compact discs, electronic or magnetic storage devices such as floppy diskettes, hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, optical disks, printer buffers, smart cards, memory calculators, electronic dialers, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

Facebook

10. Facebook Inc. is a company based in Menlo Park, California. Facebook Inc. owns and operates a free-access social networking website of the same name that can be accessed at http://www.facebook.com. Facebook allows its users to establish accounts with Facebook, and users can then use their accounts to share written news, photographs, videos, and other information with other Facebook users, and sometimes with the general public.

11. Facebook users can create profiles that include photographs, lists of personal interests, and other information. Facebook users can also post "status" updates about their whereabouts and actions, as well as links to videos, photographs, articles, and other items available elsewhere on the Internet. Facebook users can also post information about upcoming "events," such as social occasions, by listing the event's time, location, host, and guest list. In addition, Facebook users can "check in" to particular locations or add their geographic locations to their Facebook posts, thereby revealing their geographic locations at particular dates and times. A particular user's profile page also includes a "Wall," which is a space where the user and his or her "Friends" can post messages, attachments, and links that will typically be visible to anyone who can view the user's profile.

12. Facebook users can exchange private messages on Facebook with other users. Those messages are stored by Facebook unless deleted by the user. Facebook users can also post comments on the Facebook profiles of other users or on their own profiles; such comments are typically associated with a specific posting or item on the profile. In addition, Facebook has a chat feature that allows users to send and receive instant messages through Facebook Messenger. These chat communications are stored in the chat history for the account. Facebook also has Video and Voice Calling features, and although Facebook does not record the calls themselves, it does keep records of the date of each call.

FACTS SUPPORTING PROBABLE CAUSE

13. During the approximate time period of May 2020 through September 2020, an officer of the Dayton Police Department who will be referred to for purposes of this Affidavit as "Officer A" has conducted three traffic stops of vehicles driven by MALIK TAYLOR (hereinafter referred to as "TAYLOR"). TAYLOR was arrested following two of the traffic stops for drug and firearms offenses. TAYLOR was cited for traffic offenses following the third traffic stop (which occurred on or around August 27, 2020).

14. On or around September 3, 2020, Officer A assisted other officers of the Dayton Police Department in conducting a traffic stop of a vehicle parked near TAYLOR's mother's residence. The vehicle was occupied by approximately three individuals. Officers suspected, based on their past experiences, that these three individuals are associates of TAYLOR. Two of the individuals were arrested for firearms and/or drug offenses. Although TAYLOR was not present for this stop, officers suspected that he was inside of his mother's residence at the time of the stop.

15. On or around September 3, 2020, Officer A conducted a traffic stop of a vehicle driven by **WOODS**. Officers issued a traffic citation to **WOODS** for failing to stop at a stop sign. **WOODS** thereafter filed a complaint with the Dayton Police Department alleging that the traffic stop was improper. Other than this incident, Officer A has not had any other known interactions with **WOODS**.

16. In September 2020, officers of the Dayton Police Department learned that threatening communications had been posted on the Facebook website about its officers. These threatening communications were posted on the publicly available information of a Facebook account utilizing the profile name of "Richie RushLeek". The communications were posted by both "Richie RushLeek" and another individual utilizing the Facebook profile name of "Dotta Rush".

17. The profile picture and other pictures contained on the "Richie RushLeek" Facebook account appear to depict TAYLOR. The profile picture and other pictures contained on the "Dorian Woods" Facebook account appear to depict **WOODS**. Officers and an analyst from the Dayton Police Department know from previous investigations that TAYLOR and **WOODS** are associates. Officers noted that the threatening communications began on or around September 4, 2020 (one day after the traffic citation issued to **WOODS**, approximately one week after the traffic citation issued to TAYLOR, and one day after the arrest of TAYLOR's suspected associates outside of his mother's residence).

18. Below is a summary of the information posted to the "Richie RushLeek" Facebook account on or around September 4, 2020 (as viewed on the publicly available information):

a. On or around September 4, 2020, the "Richie RushLeek" account user posted a picture of Officer A that appeared to be taken from a traffic stop. "Richie RushLeek" then posted the following comment: "Can somebody tell me what I gotta do to get this cop from harassing me everyday this dude was just sittin outside my house this morning at 8am this morning while I'm taking my son to daycare somebody help me".

b. A number of other Facebook users posted comments in response to "Richie RushLeek's" posting. Included among these comments was the following, which was posted by an individual using the profile name of "Dotta Rush": "We need to set him up and kill this nigga they aint gone do shit about it but that's gone make em pay attention".

c. Later in the day of on or around September 4, 2020, the above noted posting made by "Dotta Rush" was no longer publicly viewable on the "Richie RushLeek" Facebook page. Based on my training and experience, I know that Facebook administrators monitor communications posted by Facebook users and remove any communications that incite violence. It is not known at this time if the posting was removed by "Dotta Rush", "Richie RushLeek", or Facebook administrators.

19. On or around September 5, 2020, the "Richie RushLeek" account user posted the following additional comments on his Facebook account: "Facebook police ass want let me see my notifications since I said something bout the police ass nigg *(emoticons)* Facebook", "I'm really weak asf I got like 20 notifications that I can't see since I made that post FUCK THA POLICE AND FB I GOT 200 round for a police ass mf *(emoticons)*".

20. Based on the information detailed above, there is probable cause to believe that **WOODS** and TAYLOR posted threats via their Facebook accounts to injure Officer A and other law enforcement officers. There is also probable cause to believe that **WOODS** and TAYLOR conspired to injure Officer A and other law enforcement officers. Based on my training and experience, I know that accessing Facebook accounts requires the use of the Internet and thereby affects interstate or foreign commerce.

21. Based on my training and experience, I know that individuals are increasingly utilizing cellular telephones to do their computing. Due to their portable nature, cellular telephones provide individuals with easy access to their files, social media accounts, and email accounts. Also due to their portable nature, individuals typically carry cellular telephones on their persons.

22. Review of the "Richie RushLeek" and "Dotta Rush" Facebook accounts indicate that they frequently post information to their accounts, including information about their whereabouts. Based on my training and experience, I know that these frequent postings are consistent with individuals who utilize their cellular telephones to post information onto their Facebook accounts. Based on this and other information detailed in the Affidavit, it is reasonable to believe that **WOODS** has utilized his cellular telephone to access his Facebook account (the account that was utilized to post threats to Officer A).

23. Based on my training and experience, I know that individuals involved in offenses involving interstate threats often utilize cellular telephones to plan, execute, and conceal various aspects of these offenses. In my experience, subjects involved in such offenses often conduct various Internet research related to the crimes on such devices, including but not limited to: (1) the locations of the criminal activities, (2) directions to the locations of the criminal activities, (3) background information about the victims, (4) information about the whereabouts of the victims, and (5) best practices or tips in executing the activities. Subjects may also use the Internet when conducting online purchases for instrumentalities used in the commission of the crimes, such as telephones and firearms. Individuals commonly conduct such Internet research on cellular telephones.

24. Based on my training and experience, I know that individuals communicate with co-conspirators via a variety of means, to include telephone, email, and messenger applications available on social media websites. These communications may contain material information related to the planning, execution, and concealment of the criminal activities and the instrumentalities used in the execution of the crimes. I know that individuals commonly use cellular telephones to send these types of communications. Data from text messages, email messages, and messenger applications can often be recovered during forensic examinations of cellular telephones.

25. Again based on my training and experience, I know that individuals often utilize cellular telephones and digital cameras to take pictures and videos. In my experience, subjects of criminal investigations have produced photographs and video recordings that capture instrumentalities of criminal offenses and shared these files to others via a variety of means. For example, I have been involved in investigations where individuals have photographed themselves holding firearms used in the commission of criminal offenses. Also for example, I know that individuals sometimes photograph themselves holding their cellular telephones, and these telephones sometimes are the same ones used in the commission of criminal offenses. Photographs of firearms were observed on the publicly available information of the "Richie RushLeek" and "Dotta Rush" Facebook accounts.

26. I also know, based on my training and experience, that cellular telephones sometimes store GPS data and other location information on the devices. Such GPS data and location information are materially relevant in cases involving interstate threats in that it helps to identify where the subjects were when the alleged criminal offenses transpired.

COMPUTERS, ELECTRONIC STORAGE, AND FORENSIC ANALYSIS

27. Searches and seizures of evidence from computers (including cellular telephones) commonly require agents to download or copy information from the cellular telephones and their components, or seize most or all of the devices to be processed later by a qualified computer expert in a laboratory or other controlled environment. This is almost always true because of the following two reasons:

a. Computer storage devices (including cellular telephones) can store the equivalent of thousands of pages of information. Especially when the user wants to conceal criminal evidence, he or she often stores it in random order with deceptive file names. This requires searching authorities to examine all the stored data that is available in order to determine whether it is included in the warrant that authorizes the search. This sorting process can take days or weeks, depending on the volume of data stored, and is generally difficult to accomplish on-site.

b. Searching computer systems (including cellular telephones) for criminal evidence is a highly technical process requiring expert skill and a properly controlled environment. The vast array of computer hardware and software available requires even computer experts to specialize in some systems and applications, so it is difficult to know before a search which expert should analyze the system and its data. The search of a computer system is an exacting scientific procedure that is designed to protect the integrity of the evidence and to recover even hidden, erased, compressed, password-protected, or encrypted files. Since computer evidence is extremely vulnerable to tampering or destruction (which may be caused by malicious code or normal activities of an operating system), the controlled environment of a laboratory is essential to its complete and accurate analysis.

28. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

29. There is probable cause to believe that things that were once stored on any cellular telephones utilized by **WOODS** may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or

years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' and cellular telephone's internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

30. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the cellular telephones were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence might be on any cellular telephones seized from **WOODS** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

CONCLUSION

32. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence of a crime; contraband, fruits of crime, or other items illegally possessed; property designed for use, intended for use, or used in committing a crime of violations of federal law, may be located on the person of **WOODS** and on any cellular telephones located on **WOODS'** person: 18 U.S.C. §875(c) and 18 U.S.C. §372.

33. I, therefore, respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Special Agent Andrea R. Kinzig
Federal Bureau of Investigation

SUBSCRIBED and SWORN
before me this 10th of September 2020

Sharon L. Ovington
United States Magistrate Judge